REMARKS

Claims 1-22 are currently pending in the subject application and are presently under consideration. Claims 1, 3-8, 11, 12, 14, 15, 18 and 19 have been amended as shown on pp. 2-8 of the Reply. Claims 21 and 22 are newly added. Support for the amendments and new claims may be found, for example, in the claims as originally filed and in the specification at paragraphs [0028], [0040], [0049] and [0059]-[0061].

Favorable reconsideration of the subject patent application is respectfully requested in view of the comments and amendments herein.

I. Examiner Interview

Applicant's representative thanks Examiner Hailu for the courtesies extended in the telephonic interview held November 25, 2008, the substance of which is incorporated into these remarks. Proposed amendments to the claims, and new claims 21 and 22, were discussed. No agreement was reached. Examiner Hailu stated that he would consider the proposed amendments and new claims after filing of this Reply, and an updated search.

II. Rejection of Claims 1-6, 9, 10, 13 and 17 Under 35 U.S.C. §103(a)

Claims 1-6, 9, 10, 13 and 17 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hursey et al. (US Pub. No. 2003/0074573) ("Hursey") in view of Desai (US Pub. No. 2003/0188189).

The rejection is respectfully traversed. As to independent claim 1, Hursey and Desai do not support the rejection for at least the reason that, in even in combination, they fail to disclose or suggest "a normalization module that obtains an executable script and generates a normalized signature for the executable script, wherein generating a normalized signature for the executable script comprises normalizing tokens from the executable script into normalized tokens conforming to a common format," as recited in claim 1.

The Office Action correctly recognizes that Hursey is deficient as to the noted features, but cites Desai for the disclosure absent from Hursey. However, Desai is likewise deficient.

In more detail, the Office Action cites paragraphs [0051] and [0052] of Desai in support of the rejection. However, these paragraphs do not describe normalizing tokens from the executable script into normalized tokens conforming to a common format, as recited in claim 1.

Instead, they describe formatting an event log. Clearly, an event log is not an executable script as recited in claim 1. Accordingly, claim 1 is allowable over Hursey and Desai, as are claims 2 and 6-9 for at least the reason that they depend on claim 1, as well as for the additional features they recite.

For example, claim 6 recites "wherein normalizing tokens from the executable script into a common format suitable for comparison with the at least one malware signature in the malware signature store comprises renaming tokens from the executable script according to a common naming convention." The Office Action cites paragraph [0022] of Hursey for corresponding disclosure. However, Hursey is silent regarding renaming tokens as recited in claim 6. Instead, Hursey only discloses compressing or decompressing files for purposes of comparison.

As a further example, claim 9 recites "wherein generating a normalized signature for the executable script further comprises generating a set of normalized tokens for each routine in the executable script." The Office Action alleges that Hursey's abstract has corresponding disclosure. However, as noted previously, Hursey is silent regarding tokens as recited in claim 9.

Independent claims 3, 4 and 5 include similar recitations to those of claim 1 noted above, and are consequently likewise allowable over Hursey and Desai. Claims 10, 13 and 17 are likewise allowable for at least the reason that they depend on one of claims 3, 4 or 5, as well as for the additional features they recite.

In view of the above, withdrawal of the rejection is therefore respectfully requested.

III. Rejection of Claims 7, 8, 11, 12, 14-16, 19 and 20 Under 35 U.S.C §103(a)

Claims 7, 8, 11, 12, 14-16, 19 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Hursey in view of Desai, and further in view of Milliken (US Pub. No. 2004/0064737).

The rejection is respectfully traversed. Claims 7, 8, 11, 12, 14-16, 19 and 20 depend on one of claims 1, 3, 4 or 5 and consequently are allowable over Hursey and Desai for at least reasons discussed above. Milliken relates to hashing packets to detect malicious packets, not to executable scripts, and consequently does not remedy any deficiencies in Hursey and Desai. Claims 7, 8, 11, 12, 14-16, 19 and 20 are further allowable for the additional features they recite.

For example, claims 7, 11, 14 and 16 recite a "partial match," which the Office Action correctly recognizes is absent from Hursey. As noted previously, since Milliken in no way relates to executable script, it cannot supply the disclosure absent from Hursey.

Claim 7 further recites “generate a second normalized signature for the executable script, wherein generating a second normalized signature comprises normalizing tokens from the executable script into a second common format suitable for comparison with a second normalized malware signature of known malware in the malware signature store.” As noted previously, Hursey and Desai are silent regarding normalizing tokens, and consequently are further deficient with regard to claim 7. Milliken clearly does not remedy the deficiencies in Hursey and Desai.

Claim 8 recites ”wherein normalizing tokens from the executable script into a second common format suitable for comparison with a second normalized malware signature of known malware in the malware signature store comprises normalizing tokens of the executable script into a common name according to each token’s type.” Claims 12, 15 and 19 recite similar features. Since Hursey, Desai and Milliken are silent regarding normalizing tokens as discussed previously, they are further silent regarding the features of claims 8, 12, 15 and 19.

In view of the above, withdrawal of the rejection is respectfully requested.

IV. New Claims

New claims 21 and 22 are clearly allowable of record. None of the art of record discloses a computing device configured with a process to detect malware, the process including parsing an executable script to obtain a plurality of tokens therefrom, the plurality of tokens including tokens respectively corresponding to variables and subroutines of the executable script, if a token of the plurality of tokens obtained corresponds to a variable, generating a variable token based on renaming the variable, if a token of the plurality of tokens obtained corresponds to a subroutine, generating a subroutine token based on renaming the subroutine, forming a token set from the variable token and the subroutine token, comparing the token set with a token set of a known malware script, and if there is a match, reporting that the executable script is malware, as recited in claim 21. Moreover, claim 22 is likewise allowable over the art of record for at least the reason that it depends on claim 21, as well as for the additional features it recites.

CONCLUSION

The present application is believed to be in condition for allowance in view of the above comments and amendments. A prompt action to such end is earnestly solicited.

In the event any fees are due in connection with this document, the Commissioner is authorized to charge those fees to Deposit Account No. 50-1063 [MSFTP2453US].

Should the Examiner believe a telephone interview would be helpful to expedite favorable prosecution, the Examiner is invited to contact applicant's undersigned representative at the telephone number below.

Respectfully submitted,
AMIN, TUROCY & CALVIN, LLP

/William E. Curry/
William E. Curry
Reg. No. 43,572

AMIN, TUROCY & CALVIN, LLP
127 Public Square
57th Floor, Key Tower
Cleveland, Ohio 44114
Telephone (216) 696-8730
Facsimile (216) 696-8731